BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 16 384.7

Anmeldetag: 12. April 2002

Anmelder/Inhaber: SCM Microsystems GmbH, Ismaning/DE

Bezeichnung: Conditional Access Network

IPC: H 04 L, H 04 N

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 29. April 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hiebinger

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

A 9161
06/00
EDV-L

PRINZ & PARTNER GbR

PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS
EUROPEAN TRADEMARK ATTORNEYS

Manzingerweg 7
D-81241 München
Tel. +49 89 89 69 80

12. April 2002

SCM Microsystems GmbH
Oskar-Messter-Str. 13
85737 Ismaning

Unser Zeichen: S 4808 DE
HD

Conditional Access Network

The present invention relates to a method of operating a conditional access network wherein a provider distributes valuable contents over the network and end-users are allowed to access such valuable contents in function of individual access rights defined by a user license. The invention also relates to a conditional access component for use in a conditional access network wherein a provider distributes valuable contents over the network and end-users are allowed to access such valuable contents in function of individual access rights defined by a user license.

In a conventional network for the distribution of valuable contents such as Digital Video Broadcast "DVB", the end-user is provided with a conditional access unit that is either embedded in a Set-Top-Box or constitutes a pluggable module for insertion into a Common Interface ("CI") slot of a Set-Top-Box. In either case, the conditional access unit includes a SmartCard reader for accommodation of a subscriber card, i.e. a SmartCard (a Chip card) that contains required functionality and data to control secured access to the valuable contents in conjunction with the conditional access unit.

Due to general aspects of security, such as the level of protection against intrusion, and to technical requirements such as data formats, video resolution etc., content providers use different conditional access systems, and each conditional access system requires a specific conditional access component which the end-user must acquire to gain access to contents distributed with that particular conditional access system.

The present invention provides a new way to allow an end-user to gain access to valuable contents distributed in any of a plurality of conditional access systems with just one conditional access component that has a basic functionality common to all of the plurality of conditional access systems, and that can be selectively enabled or disabled for any of the plurality of conditional access systems, ensuring at least the same level of security as in conventional DVB networks.

The invention as defined in the appending claims will be explained below in further detail, and exemplary embodiments of the invention are shown in the appending drawings.

In the drawings:

Fig. 1 is an overall view illustrating the relationship between an end-user side equipment, a number of conditional access application providers and a license provider;

Fig. 2 is a block diagram illustrating a head-end conditional access application enabler framework;

Fig. 3 is a block diagram of a conditional access component;

Fig. 4 is a flowchart illustrating essential steps of a procedure enabling the conditional access component to access contents received in a transport stream under a particular conditional access system.

Purpose of the invention:

This invention aims to allow an end-user to be authorized in consuming services from several different CA systems with the same device (contrary to the current state of the art where the device is linked to the CA). This device is then able to host one or more CA applications and one or more related authorizations, at the same time.

Glossary, definition of entities and data:

AACC	Authorized Automatic CA Configuration
ATR	Answer To Reset: data sent by a smart card when it is plugged in
CAAP	(CA application Provider) the entity that permits the secure download of CAA to the SMC.
CAA	(CA application: the code that runs within the SMC, giving access to the related CAS services.
CA_ID	Unique identifier of the CAS.
CAS	(CA system) a system that enables an end-user to access to payTV programs
CAT	CA Table, that contains the CAS descriptors (parameters, data, scripts ...).
End-user	The people that want to watch the tv and pay for that.
Firmware	all kind of binary code stored in the SMC (e.g. boot, OS, applications, drivers, ...)
Licence	This element allows the SMC to run legally the related CAA.
LO	(Licence Order) this procedure permits to an end-user to acquire from the LP the right to run a CAA, having then access to its payTV programs.
LP	(Licence Provider) this entity
LT	Licence Table, that contains the CA Licence descriptors (parameters, data, scripts, ..).

MMI	Man Machine Interface: a resource provided by the STB to the SMC to allow it to display data.
Subscription	
payTV programs	Programs scrambled under control of a specific CAS.
SC	(Service Channel) a channel that carries parameters (configuration file, data, scripts) related to each CAS
Script	a sequence of commands that are executed by the SMC
SerNo	Serial Number, unique value that identifies an entity (SmCa, SMC, ...)
SMC	Secure MultiCAS Component: It is made of one or more devices; is a secure one, able to store, run and/or handle applications & data in a secure way: it means that any element within is protected against modification and illegal access.
SmCa	Smart Card
SMC keys	secret and/or public data used for security-orineted services (e.g. integrity, authentication, confidentiality)
TS	Transport Stream
TiSe	(Timing Service) a service that provides right date and time, available either outside or inside the SMC (e.g. a clock).

Sequence of operations:

1 the end-user buys the component (SMC)

2,in parallel:

2 he retrieves the CA Application that will run on the device

2' he acquires the authorization to use such application

3 he consumes the CA services

The steps 2 and 2' could be made in any order.

Description of the different actions to be considered :

1. SMC purchasing

The end-user buys a SMC.

This device does contain at least boot firmware, able to manage security, handle smart cards, perform secure download, process licences. The SMC could also embed some other applications such as CAA (one or more). In term of data, it could embed one or more licences for one or many CAS.

2. CAA Acquisition

In this part, we develop the process used for acquiring the CA Application and the parameters needed to configure the CAS and the SMC.

Conditional Access Application means the firmware needed to process the encrypted A/V data using the different keys and licence in order to deliver a clear content to the end-user according to its rigths.

Three steps must be passed to get a CAA "pending" ready to be activated inside the SMC : CAA identification, CAA configuration and CAA acquisition.

CAS identification

1. The SMC retrieves CASs descriptors by listening the CAT on the SC (which is always available to the SMC).
2. identification is triggered by an event:
   - it could be a manual event (through MMI):The user can access a menu proposing CASs available for the end-user.
   - it could be one of the following four events:
     - SmCa insertion : If the user inserts a SmCa into the SMC, then a process of automatic CAS identification is launched.

- Module insertion or Module menu : the Module firmware can propose a set of CAAs that are identified as present and in the Service Channel, through the CAT.
- Content triggering, downstream event : If the channel selected by the user is protected by a CAS requiring a specific CAA not present as valid in the SMC, and if the considered CAA is conform to the AACC, then a new CAS is automatically identified.
- License presence (means step 2' has been already performed): If the license corresponding to a CAA is present and valid in the SMC, then the corresponding CAA is identified as required by the CAS to go on configuration phase.

At this step, the CAS has been choosen.

3. The SMC checks the presence of the corresponding CAA inside it.
4. If the considered CAA is present and conform to the latest version (using information coming from the CAT), then the CAA acquisition is considered as achieved.
5. If the considered CAA is not present or in an older version, then the CAS identification is complete.

At the end of the CAS identification, the SMC knows **CA_ID** and may have **CAA.**

CAA Configuration

Once identified, the CAA needs a lot of dynamic parameters to be set. The fact that different CASs can be loaded inside the SMC, added to a need of adaptation skill to prevent obsolecence of the architecture implies that the CAA could come with its parameters through a dedicated specific Service Channel.

The Service Channel can be a database carried by the downstream, and containing the following parameters that will allow

- the CAS to be configured and downloaded using for example a script.
- and the SMC itself to be configured to integrate the new CAA.

Some of the parameters can be used by both the CA and the SMC, and can be :

- the ATR of the SmCa in order to identify it
- The SerNo corresponding to the Smart Card or to the CA to be downloaded (including e.g. mask features for zoning)
- The script describing the method to be used to download the CAA firmware (location of data, files locations and their signature ...
- A reference to the license needed to unlock the CA.

At the end of the CAA configuration, the SMC knows **CA_ID and how and where it can get the latest version of the CAA.**

CAA acquisition

Once identified and configured, the CAA must be acquired by the SMC (e.g. by a download). At the end of this process, the CAA will be fully available to the system, but will remain locked until all the rights (especially the license) have been checked sucessfully.

The CAA acquisition can be proceeded as following :

1. The CAA can be already present in the SMC , whether because the system was sold with this CAA inside, or because this CAA was already acquired (pre-stored) in the system in a previous session. Then, its integrity and validity must be checked, and the acquisition is considered as ended.
2. The script contained in the Service channel can be ran in order to download the CAA over the air, setting the tuner on the appropriate transponder and channel, and filtering the downstream in order to collect the correct files.

At the end of the CAA acquisition, the SMC has **the latest version of the CAA relative to the CA_ID.** The CAA is in a locked state until the license and required rights have been checked as valid and up-to-date.

2'. Licence acquisition

2'0. Description of the licensing system

The CAA enabler Head End (owned by the LP) is :

- a CAA EMM builder,
- an encryption unit (ENC) and
- a database to store information like SMC identifier(SMC id), SMC addresses and SMC keys in a secure manner.

This Head End component will generate CAA EMMs (used for Licence transport) in MPEG packet format and sends these to the connected multiplex (MUX)that receives also Video/Audio data, standard EMM and ECM, Service Information (SI) and Program Service Information (PSI). In addition it transmits the CAA EMM Packet Identifier (PID) and the CA_SYS_ID to the SI/PSI generator.

The task of the SI/PSI generator is to modify the Conditional Access Table(CAT), i.e. to add a ca_descriptor() containing the CAA EMM PID and the CA_SYS_ID. The purpose is to signal the CAS where it will find the CAA EMM stream. The mechanism is identical to the one used for the EMM play out.

On the receiver side, in the SMC, the CAA enabler consists of three components:

- the CAA EMM filter,
- the verifier (a part of the firmware that is able to check EMM validity) and
- a secure storage to store SMC SerNo, SMC addresses, SMC keys and control data. This storage area is protected against unauthorized access and modification.

The CAA EMM filter extracts the CAT from the encrypted transport stream TS* and analyses it to get the PID where the CAA EMM stream is played out. The next task is to interpret the CAT to find the CAA EMM which is addressed to the specific module. If one is found the filter unit sends the CAA EMM to the verifier.

The verifier uses a SMC key to proof the authenticity of the EMM (e.g. by using digital signature feature) and in the case of a successful verification, it decrypts the CAA EMM. The next step is to process the instructions of the CAA EMM payload. In the case of an activation the SMC enables e.g. the de-scrambler to produce the clear stream TS.

2'.1 Licence Identification:

The end-user selects manually or automatically, thru the SMC, the CAS he wants to acquire. It leads for the SMC to the knowledge of the CA_ID.

It could be done in different manners:

2'.1.a insertion of the SMC, or service selection: it then triggers a select feature, thru an MMI, (e.g. using a menu and the remote control).

2'.1.b insertion of the CA smart card: it then identifies the CA_ID, as it is embedded in the smart card. This value is sent to the SMC.

2'.1.c content triggering: by choosing himself a channel or a service, the end-user selects and identifies the CAS.

At the end of this point, the SMC knows the **CA_ID**

2'.2 Licence Configuration

The SMC retrieves all parameters (e.g. fees, phone number, SerNo, licence options) associated to the CA_ID,required for Licence access, in order to perform the retrieval of the CA-licence. This information can be taken in the Service Channel (from the LT) or in a fixed database stored in the SMC.

At the end of this point, the SMC knows **where and how access to the CA licence(s).**

2'.3 Licence Acquisition:

If a return channel exists,

- the end-user processes a request to the LP for the CA-licence, to do that, the end-user, using config parameters, requests for a licence from the LP (e.g. financial transaction), bringing in the sent data everything requested by the LP (e.g. SMC SerNo, identity, ...).
- the LP sends the specific licence, after complete payment, the LP processes data specific to the end user SMC and the chosen CAA, and sends them to the SMC (e.g. EMM).

If no return channel exists

- the end user buys a prepaid card, embedding a CA-licence
- the licence is downloaded in the SMC, made specific (i.e. the licence is linked to the SMC SerNo).
- Later, when rights are used, the credits in the card are burned.

At the end of this point, the SMC has a **licence of use for a specific CAS.**

3. Consumption of PayTV programs

The end-user wants to consume programs or services. The CAA enabler feature requires some additional hardware resources on the head end component and on the SMC component. This is described in 2'0.

Here is the sequence :

3.1 the end user selects a channel or a service he wants to consume

3.2 the SMC checks the corresponding CAA (i.e. CAA(CA_ID(channel)):

(optional) checks presence of the smart card related to the CA

checks that the CAA is not corrupted and locked

3.3 the SMC checks the CA licence:

checks the licence presence

checks the licence parameters are OK (date-by using the TiSe-, identity, SerNo, ..).

3.4 the SMC runs the CAA.

5

Claims

1. A method of operating a conditional access network wherein a provider distributes valuable contents over the network and end-users are allowed to access such valuable contents in function of individual access rights defined by a user license, characterized in that the valuable contents are made available to the end-users by way of a plurality of different conditional access systems, each end-user is provided with a generic conditional access component having a basic functionality common to all conditional access systems, and particular conditional access systems are selectively enabled on each conditional access component subject to a successful verification of a corresponding license.
2. The method of claim 1, wherein the valuable contents are distributed in a digital transport stream that contains Entitlement Management Messages "EMMs" specific to each conditional access system.
3. The method of claim 2, wherein each conditional access component includes a filter unit for filtering out the specific EMMs of conditional access systems enabled on the component and a verifier unit for the verification of access rights defined by the filtered specific EMMs.
4. The method of claim 3, wherein the valuable contents in the transport stream are scrambled, each conditional access component has a descrambler adapted to process a scrambled transport stream into a clear transport stream, and the descrambler is enabled or disabled in function of a successful or unsuccessful verification, respectively, of the access rights.
5. The method of any of claims 1 to 4, wherein each conditional access system has an associated application for execution by the conditional access component.
6. The method of claim 5, wherein applications are downloaded over the network from a conditional access application provider.

7. The method of any of claims 1 to 6, wherein the network includes service channels for the transmission of configuration data to the conditional access components.

8. A conditional access component for use in a conditional access network wherein a provider distributes valuable contents over the network and end-users are allowed to access such valuable contents in function of individual access rights defined by a user license, characterized by a basic functionality common to a plurality of different conditional access systems used in the network and an enabling unit selectively enabling or disabling access by the component to valuable contents of particular conditional access systems.

9. The conditional access component of claim 8, comprising a memory for storing at least one conditional access application associated with a particular conditional access system and means for loading said application into said memory.

10. The conditional access component of claim 8 or claim 9, the valuable contents being distributed in a digital transport stream that contains Entitlement Management Messages "EMMs" specific to each conditional access system, and comprising a filter unit for filtering out specific EMMs of conditional access systems enabled on the component and a verifier unit for the verification of access rights defined by the filtered specific EMMs.

Abstract

In a conditional access network a provider distributes valuable contents such as digital TV over the network and end-users are allowed to access such valuable contents in function of individual access rights defined by a user license. The valuable contents are made available to the end-users by way of a plurality of different conditional access systems, each end-user is provided with a generic conditional access component having a basic functionality common to all conditional access systems, and particular conditional access systems are selectively enabled on each conditional access component subject to a successful verification of a corresponding license.

Fig.1

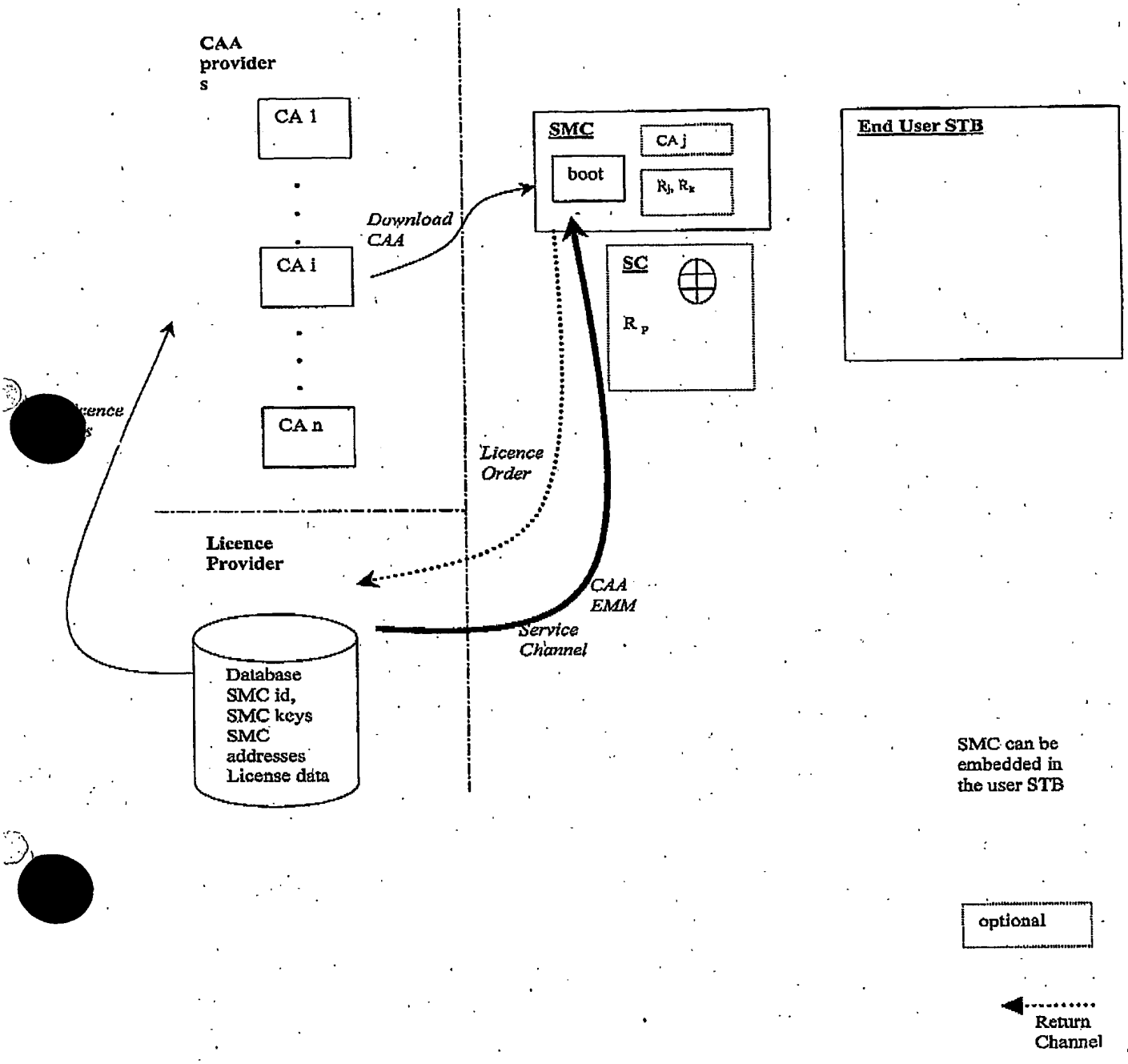
CAA provider s
CA 1
CA i
CA n
Download CAA
SMC
CA j
boot
SC
End User STB
Licence Order
Licence Provider
CAA EMM
Service Channel
Database SMC id, SMC keys SMC addresses License data
SMC can be embedded in the user STB
optional
Return Channel

Fig. 2

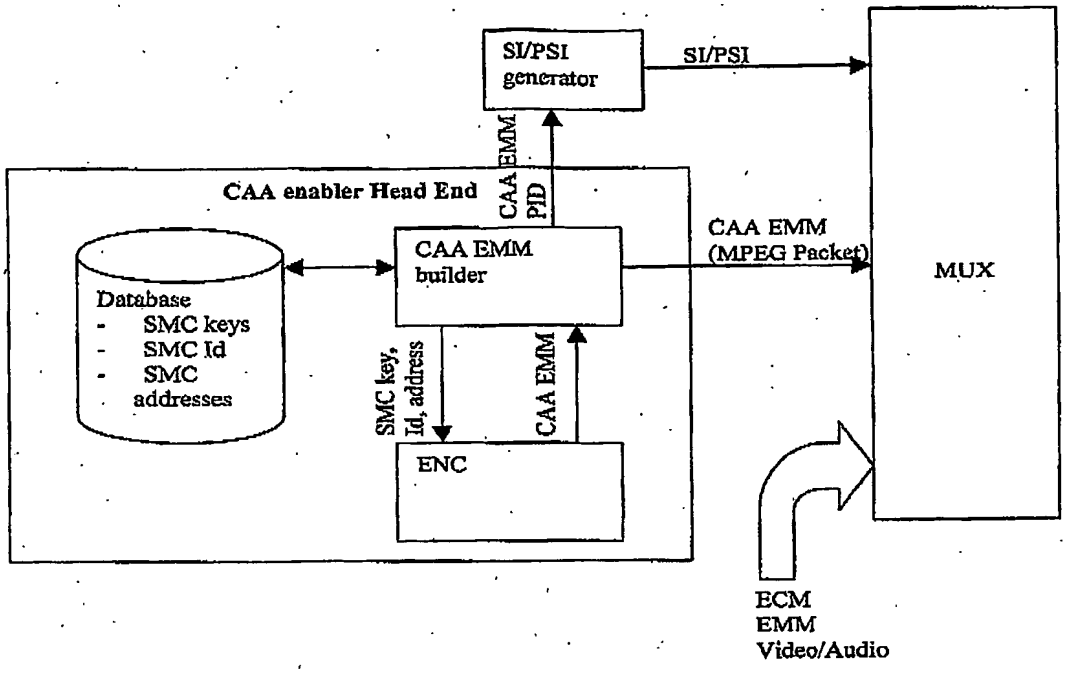
SI/PSI generator
SI/PSI
CAA EMM PID
CAA enabler Head End
CAA EMM builder
CAA EMM (MPEG Packet)
MUX
Database
- SMC keys
- SMC Id
- SMC addresses
SMC key, Id, address
CAA EMM
ENC
ECM
EMM
Video/Audio

Fig. 3

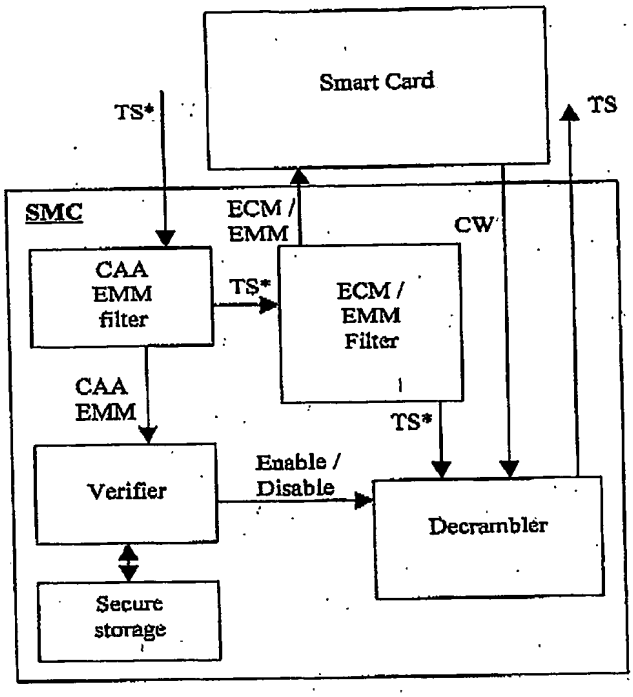
Smart Card
TS*
TS
SMC
ECM / EMM
CW
CAA EMM filter
TS*
ECM / EMM Filter
CAA EMM
TS*
Verifier
Enable / Disable
Decrambler
Secure storage

Fig. 4

Flow chart of CAA enabler on the SMC side